UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	Criminal No. 08-CR-10223-PBS
v.	)	
	)	Criminal No. 09-CR-10262-PBS
ALBERT GONZALEZ	)	
	)	Criminal No. 09-CR-10382-DPW
Defendant.	)	**REDACTED VERSION**

GOVERNMENT'S SENTENCING MEMORANDUM

The seriousness of Albert Gonzalez's computer crimes, wire frauds and identity thefts, and the profound need to provide adequate specific and general deterrence, dictate the government's recommendations of twenty-five years' incarceration in the TJX case (08-CR-10223-PBS), twenty years' incarceration in the Dave & Buster's case (09-CR-10262-PBS), and twenty-five years' incarceration in the Heartland Payment Systems case (09-CR-10382-DPW),[1]

[1] Gonzalez's uninterrupted course of computer crimes, wire frauds and identity thefts between 2003 and 2008 resulted in his being indicted in three districts: the District of Massachusetts, the Eastern District of New York and the District of New Jersey. Two of these cases are scheduled for sentencing before Judge Saris on March 25th: the TJX/OfficeMax/DSW case indicted in Massachusetts (08-CR-10223-PBS), and the Dave and Buster's case (09-CR-10262-PBS), originally brought in the Eastern District of New York and transferred here pursuant to Fed. R. Crim. P. 20. The third case is scheduled for sentencing the following day before Judge Woodlock: the Heartland/Hannaford/7-Eleven case (09-CR-10382-DPW), originally brought in the District of New Jersey and transferred here for plea and sentencing. This memorandum addresses all three cases.

Gonzalez reached separate plea agreements with the U.S. Attorneys' Offices in the three districts in which he was indicted. They differ in form as well as content. In pertinent part:

Case number 08-CR-10223-PBS, the Massachusetts case, was resolved pursuant to Fed. R. Crim. P. 11(c)(1)(C). Specifically, Gonzalez entered into a binding agreement with the United States that the appropriate disposition of the case was as sentence of imprisonment for not less than fifteen years nor more than twenty-five years.

all to be served concurrently.

If imposed, the sentences would be the longest ever imposed in an identity theft case and among the longest imposed for a financial crime, which is appropriate because Gonzalez was at the center of the largest and most costly series of identity thefts in the nation's history. He knowingly victimized a group of people whose population exceeded that of many major cities and some states – certainly millions upon millions, perhaps tens of millions. He did so at the cost of hundreds of millions of dollars to businesses ranging from small banks and credit unions[2] to Fortune 500 companies.[3] And he did so while on pretrial release from an earlier federal case and while intentionally obstructing justice. Under these exceptional circumstances, the sentence advised by the United States Sentencing Guidelines is imprisonment for life.

The Nature and Scope of Gonzalez's Criminal Conduct

To commit identity thefts on such an immense scale, Gonzalez orchestrated the efforts of people with special skills and capacities on two continents: Christopher Scott, Patrick Toey,

---

Case number 09-CR-10262-PBS, the New York case, was resolved pursuant to Fed. R. Crim. P. 11(c)(1)(B), with the sentence constrained only by the maximum term of imprisonment of the count of the Indictment to which Gonzalez pled guilty: twenty years.

Case number 09-CR-10382-DPW, the New Jersey case, was, like the New York case, resolved pursuant to Fed. R. Crim. P. 11(c)(1)(B). However, Gonzalez agreed in the New Jersey case not to seek a sentence below 17 years' imprisonment and the government reciprocally agreed not to seek one over 25 years' imprisonment. The government further agreed not to seek a consecutive sentence for Albert Gonzalez's violation of 18 U.S.C. § 3147 that results in a cumulative sentence of more than 25 years' imprisonment.

The parties have agreed that the sentences in the three cases should be served concurrently.

[2] Victim impact statement of Visa, November 30, 2009.

[3] Victim impact statement of the TJX Companies, January 19, 2010

Stephen Watt, Humza Zaman and Jeremy Jethro (all of whom have admitted to their roles, pled guilty and either been sentenced or are pending sentencing in this District); D.D., J.W. and M. Y. (who have been convicted and sentenced for related crimes in California, Pennsylvania and Turkey, respectively); and coconspirators in the former Soviet Republics known only by their pseudonyms.

In short, Gonzalez's organization:

1. Took advantage of security vulnerabilities present in numerous businesses' wireless computer networks and databases over the course of five years, from 2003 until 2008, when he was arrested;

2. Unlawfully accessed the computer networks processing credit and debit card transactions for, among other companies: BJ's Wholesale Club, DSW, OfficeMax, Sports Authority and TJX Companies;

3. Located and stole sensitive files and data on those networks, including track 2 data (the data encoded on the magnetic strips on the backs of credit and debit cards read by ATM machines and credit card readers) pertaining to tens of millions of transactions;

4. Secured a source in a former Soviet republic to decrypt encoded PIN numbers;

5. Sold track 2 data in the United States and Eastern Europe for fraudulent use;

6. Used other track 2 data directly to withdraw large sums from banks' ATM machines; and

7. Used sophisticated techniques to launder their proceeds through surrogates, anonymous web currencies, and Latvian bank accounts in the names of shell corporations.

In addition to the computer intrusions and data thefts that he orchestrated, Gonzalez assisted Russian and Ukrainian coconspirators in attacks on corporate computer networks and massive identity thefts in which they, rather than he, took the leading role. At different times, Gonzalez, alone or assisted by a member of his organization:

1. Provided his Russian collaborators access to victims' compromised computer networks;

2. Conducted network reconnaissance;

3. Supplied, modified and tested malicious software used to exploit computer systems and capture payment card information; and

4. Made secret computer servers available to his Russian collaborators to store malicious software and attack corporate victims.[4]

The Seriousness of Gonzalez's Offense

The sheer extent of the human victimization caused by Gonzalez and his organization is unparalleled. Just two of Gonzalez's computer servers contained more than forty million distinct credit and debit card numbers ("payment card numbers"). DSW reliably estimated that Gonzalez's organization stole more than 1,000,000 payment card numbers from their systems and TJX reliably estimated that Gonzalez stole more than 11,000,000 current payment card numbers from theirs.[5] Each of the payment card numbers belonged to an individual victim.

---

[4] Gonzalez's collaboration with two Russian co-conspirators in attacks on five corporate networks is the subject of the New Jersey Indictment before Judge Woodlock in case number 09-CR-10382-DPW. There is tension between the plea agreement in that case and the one in the Massachusetts case to be sentenced by Judge Saris, 08-CR-10223-PBS.

Under the terms of the plea agreement in the New Jersey case, the defendant must recommend to the Court a sentence of not less than 17 years' imprisonment; under the terms of the Massachusetts agreement he may recommend 15. The New Jersey agreement provides for harsher penalties because it was executed three months after the Massachusetts agreement when the scope of readily provable and mutually agreed upon relevant conduct had expanded, with the addition of the conduct charged in New Jersey briefly described here.

So that Gonzalez can live up to his obligations under both agreements without being required to recommend the higher sentence in both cases, it is important that Judge Saris only consider the conduct charged in the Massachusetts and New York cases when sentencing him.

[5] Outside counsel for both DSW and TJX retained expert consultants to conduct extensive forensic analyses once evidence of Gonzalez's intrusions and data thefts appeared.

The raw financial consequences identified to date – in the hundreds of millions of dollars – are five to ten times as large as those caused by any individual convicted in this District and among the largest nationwide. As a direct consequence of Gonzalez's attacks on their computer networks and theft of customers' payment card numbers, companies, banks and insurers lost close to $200 million – approximately 5,000 times the annual wage of an average American worker. Among the victims hurt the worst were DSW, which lost between $6.5 million and $9.5 million; BJ's Wholesale Club, which lost between $11 million and $13 million; and TJX, which lost more than $170 million.

Additionally, as a result of Gonzalez's collaboration with two Russian hackers, identified as "Hacker 1" and "Hacker 2" in the New Jersey indictment, approximately 130 million payment card numbers were put at risk. As a consequence, Heartland Payment Systems, the worst damaged, lost nearly $130 million.

Gonzalez Foresaw and Even Intended These Massive Losses

Gonzalez was coldly aware that his computer intrusions and identity thefts were having an enormous impact on major corporations, credit card companies, banks and countless unsuspecting individuals. Indeed, as early as 2006, Gonzalez urged his international payment card fence, Maksym Yastremskiy ("Maksik"), to quickly sell payment card numbers (in slang, "dumps") which Gonzalez had stolen from a major clothing retailer, describing what typically followed the discovery of one of his computer intrusions and identity thefts:

> [Gonzalez] i'm surprised [major retailer] wasn't on the news, every hack i've made is on the news heh
>
> * * *
>
> [Gonzalez] I hacked [major retailer] and i'm decrypting pins from their stores
> [Gonzalez] visa knows [major retailer] is hacked
> [Gonzalez] but they dont know exactly which stores are affected

[Gonzalez]	so i decrypt one store and i give to you
[Gonzalez]	visa then quickly finds this store and starts killing dumps
[Gonzalez]	then i decrypt another one and do the same
[Gonzalez]	but i start cashing with my guys
[Gonzalez]	visa then finds THAT store and kills all dumps processed by that [major retailer] store
[Gonzalez]	understand?
[Gonzalez]	its a cycle
[Maksik]	yes
[Gonzalez]	this is why i'm telling you to sell them fast fast
[Gonzalez]	also some banks just said fuck waiting for the fraud to occur, lets just reissue EVERY one of our cardholders which shopped at [major retailer] for the last 4 years

ICQ exchange logged by Maksym Yastremskiy, March 2, 2006, 9:44 p.m to 10:25 p.m. (bracketed name redacted).[6]

Acknowledging the strength of the evidence against him, in the New Jersey plea agreement, Gonzalez stipulated that it was fully foreseeable to him that:

> (1) His Russian co-conspirators in that case would use malicious software to gather and steal tens of millions of credit card numbers from their victims;
>
> (2) This theft of credit and debit card numbers would affect more than 250 financial institutions; and
>
> (3) Losses to the five corporate victims resulting from the computer intrusions and data thefts in that case alone would exceed $20,000,000.[7]

[6] Gonzalez and Yastremskiy communicated using an instant messaging protocol called "ICQ" that uses numbers to identify users. Gonzalez utilized multiple identification numbers, including 201679996, which he used in the logged chat sessions that follow. For ease of reading, his name, and that of Maksym Yastremskiy ("Maksik") have been substituted as appropriate. (Abbreviations, shorthand notations and spellings are those recorded in the original logs). All of the chat logs contained in this memorandum were obtained from computers seized from Yastremskiy, and are contained in Appendix A being filed under seal with the Court.

[7] Plea Agreement between Albert Gonzalez and the U.S. Attorney's Office for the District of New Jersey, Schedule A, ¶¶ q-s.

Gonzalez Disrespected the Courts and Intentionally Obstructed Justice

To avoid detection and capture during his massive schemes, Gonzalez repeatedly lied to and manipulated the Federal Courts, Federal law enforcement and even his own family. He was, throughout the relevant periods, on pretrial release from the Federal District Court for the District of New Jersey. Massachusetts Presentence Report ("MAPSR") ¶28, n. 4; New Jersey Presentence Report ("NJPSR") ¶28, n. 5.[8] For a significant portion of the time, he was (purportedly) assisting the Secret Service to investigate others. MAPSR ¶¶ 27-28; NJPSR ¶¶27-28. During this time, however, Gonzalez simultaneously was using sensitive investigative information he learned from the Secret Service to obstruct justice by ensuring that his co-conspirators escaped detection. For this purpose, for example, he warned co-conspirator Patrick Toey, who was selling blocks of stolen credit and debit card numbers for Gonzalez, to stay away from a Secret Service undercover Internet site as the Service's investigation drew to a close. MAPSR ¶¶ 29, 72-73; NJPSR ¶¶ 29, 94. Gonzalez even callously laundered tens of thousands of dollars in currency through his parents' line of credit, and stashed another $1.1 million in a hole in their backyard. *See* MAPSR 57; NJPSR ¶73 (describing stashed currency).

Proportional Punishment and Deterrence

Comparing the sentences that the government is recommending for Gonzalez to others imposed for similar offenses is made challenging by the comparative scale of Gonzalez's crimes and those of previous computer crimes and identity thefts inside and outside the district. But, the sentences in three significantly smaller but similar cases demonstrate why sentences of

[8] The Massachusetts Presentence Report is that prepared in case number 08-CR-10223-PBS; the New Jersey Presentence Report is that prepared in case number 09-CR-10382-DPW.

twenty years in the New York case and twenty-five years in the Massachusetts and New Jersey cases are proportional and appropriate. Brian Salcedo, to whom Gonzalez provided technical assistance in compromising the Lowe's computer system through its wireless network, was sentenced to nine years' imprisonment in case number 03-CR-53 in the Western District of North Carolina. Salcedo had stolen only a nominal amount of customers' credit card information when he was caught. While still very modest in comparison to Gonzalez, Mario Simbaqueba Bonilla had been more successful at computer crime and identity theft than Salcedo. He, too, was sentenced to nine years' imprisonment, having committed a series of computer intrusions, identity thefts, and credit card frauds victimizing approximately six hundred people in case number 07- CR- 20897 in the Southern District of Florida. The government proffered that Bonilla attempted and actually caused a loss of $1.4 million, less than one per cent of the loss caused by Gonzalez. Lastly, Max Ray Butler was sentenced to thirteen years' imprisonment in case number 07-CR-332 in the Western District of Pennsylvania after hacking into financial institutions, credit card processing centers and other secure computers in order to acquire credit card account information and other personal identification information. He provided many of these credit card numbers to an accomplice who used the cards and sold others over the Internet. Again, by way of comparison to Gonzalez's case, Butler's computers contained approximately 1.8 million payment card numbers while the parties stipulated, for Guidelines purposes, to a loss resulting from the scheme of $86.4 million dollars. The government filed a motion under U.S.S.G. § 5K1.1 on behalf of Butler, and urged the Court to impose the substantially below Guideline sentence in light of extensive and valuable cooperation provided by Butler following his arrest.

The only individuals in Gonzalez's organization, itself, to be sentenced to date are Humza Zaman (09-CR-10054-MLW) and Stephen Watt (08-CR-10318-NG), neither of whom were principals.[9] Zaman, who did not participate in any of the computer intrusions or identity thefts and acted as a courier for Gonzalez as he laundered appproximately $700,000, was sentenced to a Guidelines sentence of 46 months' imprisonment by Judge Wolf. Watt, who according to both Gonzalez and Watt edited the sniffer program used by Gonzalez in TJX without Gonzalez telling Watt its intended use but did not participate in any of the other charged data thefts or profit in any way, was sentenced to two years' imprisonment by Judge Gertner.[10] Neither of Gonzalez's principal collaborators in the United States – Christopher Scott and Patrick Toey – has been sentenced yet.[11]

Proportional treatment of defendants nationally is a core objective of federal sentencing. *See* 18 U.S.C. §3553 (a)(6); *United States v. Milo*, 506 F.3d 71, 76 (1st Cir. 2007); *United States v. Ahrendt*, 560 F. 3d 69, 77 (1st Cir. 2009) ("[S]ection 3553(a)(6) aims primarily at the minimization of disparities among defendants nationally," quoting *United States v. Martin*, 520 F. 3d 87, 94 (1st Cir. 2008)). Brian Salcedo, Mario Simbaqueba Bonilla and Max Ray Butler all committed crimes similar in nature to that for which Gonzalez presently is being sentenced.

---

[9] Jeremy Jethro, who sold malicious software to Gonzalez, is scheduled to be sentenced on March 22, 2010. However, Jethro had no involvement in any of the TJX, Dave and Buster's or Heartland series of intrusions and data thefts.

[10] While the government agrees that Watt was less culpable than Gonzalez, Christopher Scott and Patrick Toey, the government respectfully disagrees with Judge Gertner's finding that Watt was "less culpable than all the other participants" and strongly disagrees with the sentence she imposed.

[11] Christopher Scott is scheduled for sentencing before Judge Woodlock on March 29th; Patrick Toey before Judge Young on April 15th.

Because Gonzalez's crimes eclipsed theirs in size and were far more pernicious, a 25-year sentence for Gonzalez would further 18 U.S.C. § 3553(a)'s goal of proportionate sentencing.

[SECTION REDACTED]

Gonzalez Appreciated the Utility of Interpersonal Relationships, as Well as Calculated Business and Data Theft Plans, Making His Claim of Diminished Capacity Dubious at Best

Before Gonzalez was arrested in this case, he was never hospitalized for psychiatric concerns, diagnosed with a mental health condition or prescribed psychiatric medication, and he had not even met with a psychiatric professional. Yet, just before the original sentencing date with Judge Saris, Gonzalez hired a doctor to examine him, who opined that "many elements of Mr. Gonzalez's experience and behavior are consistent with description [sic] of the Asperger's disorder" and that he met "criteria for Internet Addiction," which purportedly "exerted devastating influences" on Gonzalez's "capacity to knowingly evaluate the wrongfulness of his actions and consciously behave lawfully and avoid crime." Letter from Dr. Barry H. Roth, Sentencing Memorandum of Albert Gonzalez, Exhibit C, p.4.

Little weight should be given to these opinions. The defendant's expert does not describe the accepted criteria for Asperger's Disorder he found in Gonzalez, nor does he explain why, in their absence, he made the diagnosis. Similarly, he does not describe the criteria he used when making a diagnosis of "Internet Addiction," a mental illness neither widely recognized nor found in the Diagnostic and Statistical Manual of Mental Disorders. In neither case does he (nor can he) justify the linkage between the alleged disorders and Gonzalez's sophisticated scheme to hack into corporate computer networks, steal credit and debit card numbers, sell them internationally, and launder the proceeds. Further, to the extent Gonzalez's psychiatrist relies in his opinions on Gonzalez's recreational use of drugs or alcohol, the United States Sentencing

Commission explicitly has rejected drug use as a grounds for reducing a defendant's sentence. U.S.S.G. § 5K2.13 ("[T]he court may not depart below the applicable guideline range if (1) the significantly reduced mental capacity was caused by the voluntary use of drugs or other intoxicants.") Gonzalez repeatedly, and strenuously, objected to being interviewed and examined by any psychiatrist other than the one whom he retained. When the Court ordered him to submit to an independent examination, he continued to refuse to permit any questions from any psychiatrist other than his own about why he committed the crimes to which he has pled guilty.

Gonzalez's psychiatrist's report is substantially outweighed and undermined by the report of Dr. Mark J. Mills, a copy of which is attached. Of the two alleged disorders, only one, Asperger's, has a medically accepted set of diagnostic criteria. Report of Examination of Mark J. Mills, JD, MD ("Mills Report"), attached as Appendix B, pp. 4, 8. Gonzalez's behavior, both as historically related by him and presently with others, does not meet the accepted diagnostic criteria for Asperger's Disorder, methodically applied. Mills Report, p. 6. Gonzalez, to his credit, is engaging, self-aware and personable. His facility with casually meeting and engaging women (and men) is antithetical to that usually ascribed to those with Asperger's. He appreciates the utility of social relations, and is able to empathize with the anger of others (such as his girlfriend, on occasion), and feel apparent contrition for his treatment of them, again significantly weakening the possibility of an Asperger's diagnosis. Mills Report, p. 5. Finally, although Gonzalez refused to discuss the subject with Dr. Mills, his leadership of a group of hackers, data thieves and money launderers makes a diagnosis of Asperger's virtually impossible. Those with Asperger's are almost by definition not leaders. Instead they are

followers, often perceived as peripheral, isolated and strange. Mills Report, p. 6.

Gonzalez's psychiatrist's diagnosis of "Internet Addiction" is similarly baseless. There are no generally accepted criteria for diagnosing "Internet Addiction" that has met the rigors for inclusion in the American Psychiatric Association's Diagnostic and Statistical Manual of Mental Disorders. Mills Report, p. 6. And even when those who have observed patterns of "Internet addiction" describe them, the patterns they describe have fallen broadly into three groups: gaming, sexual interests and chatting/e-mailing, not computer hacking, identity theft and money laundering. *Id.***;** ***see*****,** ***e.g.,*** Sentencing Memorandum of Albert Gonzalez, Exhibit A, p. 1. Gonzalez, himself, explained that he loved the challenge posed by Internet security and that for him, the computer was an essential tool of his trade. Mills Report, pp. 6-7.

Gonzalez's spurious claims of Asperger's and "Internet Addiction" are belied by instant messaging exchanges between Gonzalez and the principal fence of his stolen payment cards, Maksym Yastremskiy ("Maksik").[12] His unguarded, contemporaneous conversations about his business demonstrate Gonzalez to be a calculating businessman, fully engaged with people around him, intensely interested in "the good life," and understanding of the consequences of his actions. He was not a psychologically incapacitated lost soul. The directness of the exchanges also belies the notion that Gonzalez was constantly intoxicated or strung out on drugs while keyboarding.

Gonzalez agreed repeatedly to a 50/50 split with Maksyk – Gonzalez would provide the database (referred to simply as "db" or "base") of payment card numbers (referred to as "dumps"), Maksik would sell them and the two would split the proceeds down the middle.

---

[12] *See* note 6, *supra*, for further details transcripts of Gonzalez's chats with Yastremskiy.

[Maksik] how much you expect to get at all from this base? do u have thoughts maybe on this matter?
[Gonzalez] i expect sales to be good for at least 3 months then die off by late spring
[Maksik] im just asking because maybe u will tell me that u want at least, for example, 2 millions $, lol, and as i will not be able to guarantee that, i would refuse
[Maksik] so what do we decide?
[Gonzalez] what % do you pay your current suppliers?
[Maksik] 50
[Gonzalez] ok
[Gonzalez] how do you pay them?
[Gonzalez] how often do you pay them
[Maksik] usualy Sunday[13]

Gonzalez was stealing and selling payment cards for a purpose: he wanted to make money, and lots of it:

[Gonzalez] same here, I rather stay home and make money, I have a goal... I want to buy a yacht
[Gonzalez] like Roman Abramovich[14]

* * *

once I reach my goal I won't be doing anything illegal... laundering money if done correctly flies under LE radar

* * *

15 million is what I want to have total before I start moving to 2nd phase of laundering it[15]

When sales went well, Gonzalez was pleased:

[Gonzalez] how are sales?
[Maksik] Total 456,00 68400,00 [456 payment card numbers for which

[13] ICQ exchange logged by Maksym Yastremskiy on November 22, 2006, 2:45 p.m. to 2:55 p.m.

[14] ICQ exchange logged by Maksym Yastremskiy on March 7, 2006, 8:17. Roman Abramovich, one of the world's richest men, is famously in a competition for ownership of the world's largest yacht.

[15] Gonzalez IBM laptop, pagefile.sys.file.

> Gonzalez's share is $68,400.00 at $150 apiece; a comma is used by Yastremskiy in the place of a decimal point throughout]
> [Gonzalez] :) [16]

When sales went less well, as when there was an oversupply in the marketplace or particular banks saw patterns of fraud on their payment cards and closed blocks of affected accounts, Gonzalez sought to limit losses:

> [Gonzalez] any new stats there?
> [Maksik] so far, total 182,00 27300,00 [182 cards; $27,300.00] but 8 big order are not confirmed
> [Gonzalez] thats kinda shitty
> [Maksik] I have a lot for sale still
> [Gonzalez] would be smart to sale them faster or all that bofa [Bank of America] will be dead man
> [Maksik] this amount is for 4 confirmedorders [sic]only
> [Gonzalez] ahh ok[17]

Gonzalez's expert seeks to paint Gonzalez as short-sighted and compulsive. He was, in fact, carefully calculating. For example, when Gonzalez believed General Dynamics, the computer forensic experts whom TJX hired when they discovered his intrusion into their systems, had just missed catching him with a "0day" attack, an attack which tries to exploit generally unknown computer vulnerabilities, he evaluated the risks and decided to shut down further efforts there:

> after those faggots at general dynamics almost owned me with 0day while I was owning tjx I don't want to risk anything[18]

---

[16] ICQ exchange logged by Maksym Yastremskiy May 20, 2006, 11:36 a.m. to 11:37 a.m. (bracketed explanatory text added; additional recorded text after symbol for smiling face omitted).

[17] ICQ exchange logged by Maksym Yastremskiy March 31, 2006, 8:57 p.m. to 9:08 p.m. (bracketed explanatory text added).

[18] Gonzalez IBM laptop computer, pagefile.sys file.

Gonzalez tried in a variety of ways to optimize his profits. Until early 2006, Gonzalez and his coconspirators would regularly "cash out" stolen payment card numbers by using the card numbers to withdraw large blocks of cash at ATM machines. Again, far from being bound by restrictive and repetitive behavior as a person with Asperger's Disorder or an addiction would be, Gonzalez recognized how much more profitable (and safer) it was to sell the card numbers, and adjusted his business model accordingly:

[Gonzalez]	ok good - do you have approximate amount total $ needed to be sent to me?
[Maksik]	well, because of some orders are pending, I can tell you approximately
[Maksik]	I have so far around 100k for you [$100,000]
[Gonzalez]	:)))
[Maksik]	and from what I have left, it should be around 15-20k more [$15-20,000 more]
[Gonzalez]	I think selling this information is better for me instead of dealing with cashers[19]

With impressive sophistication, Gonzalez sought to launder his profits with minimum expense:

[Gonzalez]	I prefer wmz over egold
[Gonzalez]	in preference order - wire, wmz, egold[20]
[Maksik]	u26 have cashier in CA, and he is cashing from ATM as he told me
[Maksik]	about egold - u want me to use an exachanger? [sic]
[Gonzalez]	how much will it cost to do egold => wmz?
[Maksik]	sec
[Maksik]	1.00 E-gold (USD) 0.9223 WebMoney (WMZ)
[Gonzalez]	thats cheap, is this roboxchange?[21]
[Gonzalez]	1%?
[Maksik]	8%

[19] ICQ exchange logged by Maksym Yastremskiy February 3, 2006, 10:02 p.m.to 10:04 p.m. (bracketed explanatory text added).

[20] WMZ, or WebMoney, and egold are both offshore, Internet based payment systems.

[21] Roboxchange is an e-currency exchange service.

[Maksik] not cheap
[Gonzalez] you sure its 8%? I give 1 dollar egold and receive 0.90
[Gonzalez] which exchanger is this?
[Maksik] u give 1$, and receive 0.92
[Maksik] www.exchange.net.ua
[Gonzalez] exchange.net.ua doesn't have much wmz at times unless you're like premium customer
[Maksik] robox have 10% for exchange
[Gonzalez] its not worth it for me to do business with u26, I make more money and without headache from you... btw exchange that egold to wmz
[Gonzalez] it cost me ~12% to cashout egold
[Gonzalez] cost me 0% to cashout wmz[22]

Far from being impulsive, Gonzalez planned and worked with deliberation over extended periods of time to sell subsets of the stolen card numbers. Gonzalez, himself, urged his coconspirators to be patient as their plans reached fruition. Gonzalez's biggest early business coup was to steal a large payment card database from OfficeMax ("omx") complete with associated PIN numbers. It took a lot of time to find someone to decrypt the PIN numbers. Here, he counseled Maksik, with whom he had a continuing relationship, to show some patience.

[Gonzalez] i have 11 million
[Gonzalez] i've decrypted already almost 1 million
[Maksik] so what happend with them ?:) why its going to be 0 soon ?:) if not a secret
[Gonzalez] many have expired
[Gonzalez] data was downloaded 2003 - 2004
[Maksik] so 10 millions are expired?[23]

* * *

[Gonzalez] have patience please :) it took me 2 years to open pins [PIN numbers] from omx

---

[22] ICQ exchange logged by Maksym Yastremskiy April 13, 2006, 12:20 p.m. to 2:38 p.m. (bracketed explanatory text added).

[23] ICQ exchange logged by Maksym Yastremskiy April 13, 2006, 12:52 p.m. to 12:54 p.m.

[Maksik] ok np ;-)
[Gonzalez] 2 years from the time I hack them, to download all data, the to find proper decryption method[24]

Even if Gonzalez evidenced criteria of Asperger's, which he does not, or even were "Internet Addiction" a recognized psychiatric disorder, which it is not, no diagnosis of restricted, repetitive and stereotyped behaviors could explain or justify, medically or legally, Gonzalez's criminal behavior. Gonzalez would have the Court lose sight of the fact that he is being sentenced for organizing and directing a sophisticated group stealing credit and debit card numbers; "cashing them out"; selling them through "carders" internationally; and laundering the proceeds of the sales through shell bank accounts in Latvia, currency exchangers and straws. He is not being sentenced for using his computer repetitively or excessively (or compulsively checking his e-mail on his Blackberry).

Probation Correctly Calculated the Amount of Loss Under U.S.S.G. §2B1.1, But the Scope of the Loss and Victimization Caused by Gonzalez Is Unprecedented No Matter How It Is Calculated

The amount of loss is a specific offense characteristic in cases involving stolen credit and debit card numbers. U.S.S.G. § 2B1.1(b)(1). Loss is defined as being the greatest of actual loss or intended loss. U.S.S.G. § 2B1.1, Application Note 3(A). The First Circuit has held that, in the case of stolen credit cards, intended loss reasonably may be found to be the stolen payment cards' aggregate credit limit, since it is natural and probable to expect that purchasers of the stolen card numbers will charge as much as possible to them.[25] *U.S. v. Alli*, 444 F.3d 34, 38-39 (1st Cir. 2006)

[24] ICQ exchange logged by Maksym Yastremskiy May 27, 2006, 10:16 a.m. to 10:17 a.m.

[25] The defendant argues that he should not be held accountable for all of the credit and debit card numbers because the government cannot establish that he had sold all of them yet.

(applying intended loss of $88,500 to the theft of twelve credit cards by postal employee where he was to be paid $150 for each one, at most). It is also reasonable to hold a defendant accountable for the amount of loss as measured by the aggregate credit limit, even though the defendant's personal profit has been dramatically less. *Id*. If it were possible to calculate the aggregate credit limit here, which it is not because of the enormous number of card numbers Gonzalez stole, the loss figure would likely be far greater than that in the PSR. As a default, under the Guidelines, loss is set at a minimum of $500 per credit or debit card number. U.S.S.G. § 2B1.1, Application Note 3(F)(I). The Probation Department correctly applied U.S.S.G. § 2B1.1 and Application Note 3(F)(I) in the present case, finding the loss for Guidelines purposes exceeded $400 million, the final specific offense characteristic benchmark under U.S.S.G. § 2B1.1(b).

Gonzalez's Guideline numbers are so high because, quite literally, the impact of the white collar crime at which Gonzalez was the center is one of a handful which have been off the scale in the past two decades since the inception of the Guidelines. He finds himself at the top of U.S.S.G. § 2B1.1 (b)(1)'s specific offense characteristic chart because he stole such an unprecedented number of credit and debit card numbers, not, as he argues, because the $500 baseline contained in Application Note 3(F)(i) grossly distorts the application of the Guidelines in this case. As the First Circuit held in *Alli, supra*, it is reasonable to measure the intended loss in credit and debit card cases as the credit limit on those cards. The average credit limit of more than $9,000 per card in the *Alli* case demonstrates the reasonableness of the Application Note's default of a minimum of $500 per card, applied by the Probation Department here. *See also*

The reasoning of the court in *Alli* applies equally here: it is natural and probable to assume that he intended to continue to sell the payment card numbers he had stolen, even if his arrest prevented him from fully doing so.

United States v. Harris, 2010 WL 432399, at *11 (5th Cir. Feb. 9, 2010) (district court did not err in determining intended loss of individual who received $2,000 for 557 credit card numbers by adding the aggregate credit limit of $2,545,287.25 for 339 credit cards of which the credit limits were known, to $104,000.00, which represented a $500 loss for each of the 208 cards for which credit limits were not known). However, even if the Court were to reject §2B1.1, Application Note 3(F)(i), apply a loss of only a tenth as much, and apply that loss to only the minimum number of current, unexpired payment cards known to have been stolen from TJX and DSW (ignoring those stolen from OfficeMax, BJ's and others), the resulting loss for Guidelines purposes would remain $600 million ($50 x (11,000,000 + 1,000,000)) – well over § 2B1.1's final $400 million benchmark. Similarly, were the Court to apply the Guidelines loss, as Gonzalez suggests the Court should, to only 13% of the current, unexpired payment card numbers which he stole, the resulting loss for Guidelines purposes would remain $780 million ($500 x (13% of 12,000,000)) – again well over § 2B1.1's final $400 million benchmark. Indeed, were the Court to ignore the theft from TJX altogether and simply apply § 2B1.1, Application Note 3(F)(i) to the more than one million payment cards stolen from DSW by Gonzalez, the result would be more than $500 million ($500 x 1,000,000+).

Gonzalez seeks to move the Court from the U.S. Probation Department's wholly proper use of U.S.S.G. § 2B1.1, Application Note 3(F)(i) to actual loss to the corporate victims of Gonzalez's crimes and from there to challenge the integrity of the reported losses. He is forced to challenge the reported losses because even were the Court solely to apply actual reported corporate losses (and not apply § 2B1.1, Application Note 3(F)(i)), Gonzalez's offense level would be reduced only by 4 levels in the case before Judge Saris and 2 levels in the case before

Judge Woodlock (where there are additional relevant corporate losses), resulting in advisory Guidelines levels of 50 (54-4) and 51 (55-4), respectively, still advisory life sentences.

The impacts of Gonzalez's intrusions and payment card number thefts were sufficiently great that TJX, BJ's Wholesale Club, DSW, OfficeMax, Heartland Payment Systems and Hannaford were all required to report them in filings with the Securities and Exchange Commission.[26] Accordingly, the corporate victims were required to determine and report their losses in accordance with generally accepted accounting standards. Further, when submitting their filings to the SEC, each of these established corporations, their principals and their counsel were doubtless aware that misleading statements could be met with severe civil and criminal penalties. *See, e.g.*, 18 U.S.C. §1350 (requiring chief executive officers and chief financial officer to submit statements with each periodic SEC report affirming the accuracy of the reports).

TJX, among others, has filed a victim impact statement, representing to the Court those losses directly attributable to the defendant's intrusion into, and massive identity theft from, its computer networks. The victim impact statement enables the Court to separate those losses already incurred from those that are likely but that TJX has not yet incurred. The Victim Impact Statement also refutes the defendant's claim that his criminal conduct did not cause all of the losses suffered by TJX's shareholders and formally reported to the SEC:

> As required by and consistent with applicable accounting standards, TJX has estimated its total cost related to the Computer Intrusion in its quarterly and annual financial statements filed with the Securities and Exchange Commission. As of

[26] Pointing to an arbitrary two year period, Gonzalez argues that TJX actually profited as a result of his intrusion and data theft, with shares rising dramatically. In the ten weeks following TJX's initial announcement of the intrusion and data theft, however, as investors adjusted to the news, TJX shareholders lost over a billion dollars in equity (while the S&P 500 as a whole had fallen less than 1%).

> October 31, 2009, TJX estimated those costs as $171.5 million, at which date $146.3 million had been expended and $25.2 million had not yet been spent but was reasonably probable and estimable.
>
> * * *
>
> The total costs reflect only cash costs resulting directly from the Computer Intrusion that were incremental to costs TJX would otherwise have incurred. The total costs do not reflect the very substantial costs of TJX's own personnel in dealing with the Computer Intrusion. The total costs are net of insurance recoveries received by TJX.

Victim Impact Statement of TJX Companies, Inc., pp. 3-4. Heartland Payment Systems similarly has submitted a victim impact statement representing that they suffered nearly $130 million in losses which have been or are expected to be incurred as a direct result of the intrusion into their processing system. Victim Impact Statement of Heartland Payment Systems, pp. 2, 4.

Gonzalez blames TJX, the victim, for unquantified portions of the harm his computer intrusion and data theft caused. Gonzalez argues that he should not be held responsible because TJX, and by extension each of eight other corporate victims described in the Indictment, had sufficiently vulnerable computer networks and data protection that he and his organization could break in and steal payment card numbers.[27] As many times as Gonzalez repeats that he is not blaming the victim of his crime, that is, of course, precisely what he is trying to do.[28]

---

[27] For example, Gonzalez seeks to use the First Circuit's opinion in *In re TJX Companies Retail Security Breach Litigation*, 564 F. 3d 489 (1st Cir. 2009) to blame TJX for the losses resulting from his intrusion and data theft. This opinion, however, only addresses whether parties had standing and, if what they alleged was true, the question of whether they had stated various causes of action. Indeed, the court emphasized that it was not considering the merits of the allegations at all, in the parenthetical omitted by Gonzalez in the ellipse in his quotation from the case: "If the charges in the complaint are true (and obviously the details matter). . ." Id. at 496.

[28] A victim's conduct, while not affecting the loss for the purposes of determining a defendant's specific offense characteristic from the Guidelines' loss table, indeed may be a basis

Conclusion

Albert Gonzalez was motivated by ego, challenge and greed and was proud of the national attention his computer intrusions and data thefts drew. They drew that attention because they victimized more people than anyone had ever done before in this country, caused hundreds of millions of dollars in losses, and shook the public's trust in the security of credit and debit card transactions at some of the country's largest institutions.

Gonzalez already has been given a second chance. He used that second chance not to straighten out his life, but to provide cover as he committed ever more brash and destructive crimes. An obsession with computers – if Gonzalez had one, rather than merely viewing computers as a tool of his profitable trade – provides no justification whatsoever for his crimes. Countless people, teenagers and adults alike, spend untold hours on their computers and Blackberries without committing crimes. And virtually everyone in MIT's Department of Electrical Engineering and Computer Science could, like Gonzalez, be diagnosed as having the same obsession since childhood with computers, the same preference for communicating with others online, and the same pride in their accomplishments with their computers. Yet none chose to leverage their computer skills into massive theft and fraud.

---

for a departure if the loss calculation overstates the seriousness of the offense. *United States v. Maldonado-Montalvo*, 356 F.3d 65, 69 (1st Cir. 2003). "Theoretically, such a loss overstatement may occur where, *inter alia*, '[a]ny portion of the total loss sustained by the victim [is] is a consequence of factors *extraneous to the defendant's conduct*.'" *Id.* at 69 (quoting *United States v. Reeder*, 170 F.3d 93, 109 (1st Cir. 1999))(citations omitted, emphasis in the original). However, here, no extraneous factors increased the number of credit and debit cards which Gonzalez stole and continued to "cash out" or sell. Similarly, no extraneous factors amplified how extensively issuing banks and credit card companies reacted, the number of innocent cardholders affected, the resulting losses which had to be borne by them or passed back to victim retailers and the potentially devastating harms to retailers' businesses caused by the publicity surrounding Gonzalez's massive break-ins and payment card thefts, as evidenced by Gonzalez's knowledgeable discussion with Maksik, *supra*, at p. 6.

For the reasons set forth above, the Court should sentence Albert Gonzalez to twenty-five years' incarceration in the Massachusetts case, twenty years' incarceration in the New York case, and twenty-five years' incarceration in the New Jersey case, to be served concurrently.

Respectfully submitted,

CARMEN M. ORTIZ
United States Attorney

By: */s/ Stephen P. Heymann*
STEPHEN P. HEYMANN
Assistant U.S. Attorney

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

/s/ Stephen P. Heymann
STEPHEN P. HEYMANN
Assistant U.S. Attorney

Date: March 18, 2010